Giving data adequate protection

KUALA LUMPUR: Personal data protection is expected to get a major boost when the Personal Data Protection Act comes into force in June.

The act, which was passed by parliament in May 2010, and gazetted in June the same year, will safeguard all aspects of personal data related to commercial purposes.

Those who abuse the information obtained are liable to be fined not more than RM500,000 and jailed a maximum of three years, depending on the types of offences.

Under this act, several new offences come into existence and they are different from crimes committed under the Penal Code.

Among the offences are data-selling, failure to register data, unlawful collection of data, transfer of data without adequate protection, data-disclosure without consent, data-processing after registration has been revoked and contravening data-protection principles.

Prof Abu Bakar Munir, a lecturer at Universiti Malaya's Law Faculty, tabled a working paper on the act during a recent seminar to boost public awareness about data protection.

"I was involved in helping Singapore draw up a draft for the act to be used there soon. As for the Personal Data Protection Act 2010, I was given the trust to be the adviser."

This act covers seven principles: General Principle, Notice and Choice Principle, Disclosure Principle, Security Principle, Retention Principle, Data Integrity Principle and Access Principle.

"This act protects the data subject or individuals who own the data," he said.

Abu Bakar explained offences that can be prosecuted under this act are provided under section 40 (3) – processing sensitive data – and 38 (4), which is processing data after consent has been withdrawn.

Similar acts have been legislated in other Asian nations, including South Korea and Taiwan.

WHAT IS PERSONAL DATA?

Under section 4 of the Personal Data Protection Act (PDPA), personal data refers to any information concerning commercial transactions stored or recorded, and which can be managed automatically or as a file system.

It does not matter whether the information is being processed, stored automatically or filed by any party. But it will only be an offence if the information data is used commercially.

Personal data has a very wide scope, covering sensitive and personal information such as blood type, health records and descriptions, political and religious beliefs, mental or physical conditions, or any other data needed by the authority from time to time.

Normal personal data also involves details on bank accounts, credit cards, telecommunication links such as telephone or any other information stipulated by the act.

The lists of personal data under the PDPA can be expanded by the Authority.

However, details or information of one's credit ratings are put under the Credit Rating Agency Act 2010 and thus are not covered by the PDPA.

It should also be stressed that the PDPA comprises seven key principles that must be adhered to to protect the integrity of personal data.

SEVEN PRINCIPLES

A user is not allowed to process the personal data of another user without permission.

The user must comply with the Principle of Notice and Choice in which the information and purpose of the preliminary communication are conveyed to the data subject.

The Principle of Disclosure spells out the need to disclose the use of personal data.

The Principle of Security states that when processing personal data of any subject, precautionary measures must be taken so that the data is safe, and not tampered with, abused, missing or given to irrelevant parties.

The Principle of Storing specifies that any personal data shall not be kept in a processing system longer than needed.

For the Principle of Data Integrity, all personal data must be accurate, complete, clear and up-to-date, in line with the purpose of storing and processing.

As for the Principle of Access, a user must be given access to his/her own personal data that is kept by another user, and to be allowed to update the data.

With these principles in place, users and e-commerce practitioners will be more confident that their personal information is well protected.

In the meantime, a practical and reasonable code of practice can be formulated by private efforts or on the initiatives of the personal data commissioner.

Newly-appointed Personal Data Protection Department director-general Abu Hassan Ismail said the department accepted the challenges in implementing the act. – Bernama